des congruences où figurent des nombres non premiers au module que les nombres h_1 et k_1 seront complètement déterminés.* Cela étant ainsi, je pose

$$x_m \equiv y_m + h_1 - k_1 \quad (\text{mod. } t)$$

et par suite

$$y_m \equiv x_m + k_1 - h_1 \quad (\text{mod. } t)$$

le nombre m étant tout nombre de la suite

$$1, 2, \ldots . n.$$

De cette manière je fais correspondre à chaque solution de la congruence

$$x_1 + x_2 + \ldots . x_n \equiv h \quad (\text{mod. } t)$$

une solution bien déterminée de la congruence

$$y_1 + y_2 + \ldots . y_n \equiv k \quad (\text{mod. } t)$$

et inversement.† Les deux congruences auront donc le même nombre de solutions. Ce nombre est d'ailleurs facile à évaluer. En effet, le nombre des expressions telles que

$$x_1 + x_2 + \ldots . x_n$$

différant entre elles au moins par un des nombres qui figurent dans la somme, étant égal à

$$\frac{t!}{n!\,(t-n)!}$$

on obtiendra le nombre cherché en divisant $\frac{t!}{n!\,(t-n)!}$ par t, ce qui donne

$$\frac{(t-1)!}{n!\,(t-n)!}.$$

J'aborde maintenant une congruence telle que

$$x_1 + x_2 + \ldots . x_n \equiv h \quad (\text{mod. } t)$$

où

$$x_1, x_2, \ldots . x_n$$

sont des nombres de la suite

$$1, 2, \ldots . t-1$$

et je désigne par $\chi_h^{(n)}$ le nombre de ses solutions. Quand $n > 1$, toute solution de la congruence

$$x_1 + x_2 + \ldots . x_n \equiv h \quad (\text{mod. } t)$$

où

$$x_1, x_2, \ldots . x_n$$

* Disquisitiones arithmeticae, art. 26. † Ibid. art. 3.

font partie de la suite

$$0,\ 1,\ 2, \ldots . t-1$$

est *soit* une solution de la congruence

$$x_1 + x_2 + \ldots . x_n \equiv h \qquad (\text{mod. } t)$$

où les indéterminées ne peuvent pas prendre la valeur 0, *soit* par la suppression de l'indéterminée qui est égale à zéro, une solution de la congruence

$$x_1 + x_2 + \ldots . x_{n-1} \equiv h \qquad (\text{mod. } t)$$

où les indéterminées ont encore des valeurs différentes de zéro. L'inverse ayant aussi lieu, on aura

$$\chi_h^{(n-1)} + \chi_h^{(n)} = \frac{(t-1)!}{n!\,(t-n)!}$$

pour $n > 1$.

Or on obtient immédiatement

$$\chi_0^{(1)} = 0$$

et

$$\chi_h^{(1)} = 1$$

pour $h > 0$; on aura donc

$$\chi_0^{(n)} = \frac{(t-1)!}{n!\,(t-n)!} - \frac{(t-1)!}{(n-1)!\,(t-n+1)!} + \ldots . + (-1)^{n-2} \frac{(t-1)!}{2!\,(t-2)!}$$

et*

$$\chi_h^{(n)} = \frac{(t-1)!}{n!\,(t-n)!} - \frac{(t-1)!}{(n-1)!\,(t-n+1)!} + \ldots . + (-1)^{n-2} \frac{(t-1)!}{2!\,(t-2)!} + (-1)^{n-1}$$

d'où

$$\chi_h^{(n)} = \chi_0^{(n)-(-1)^n}.$$

Cela étant ainsi, on aura

$$f_n \equiv \chi_0^{(n)} + (a + a^2 + \ldots . a^{t-1})\,\chi_h^{(n)} \equiv (-1)^n + X(a)\,\chi_h^{(n)} \equiv (-1)^n \qquad (\text{mod. } u).$$

Comme on a d'ailleurs

$$f_{t-1} = \prod_{h=1}^{h=\frac{t-1}{2}} a^h a^{t-h} \equiv 1 \qquad (\text{mod. } u)$$

on aura

$$(x-a)(x-a^2) \ldots . (x-a^{t-1}) \equiv X(x) \qquad (\text{mod. } u)$$

* La sommation donne

$$\chi_h^{(n)} = \frac{\dfrac{(t-1)!}{n!\,(t-n-1)!} - (-1)^n}{t}.$$

dans ce sens que tout coéfficient de $X(x)$ sera congru au coefficient correspondant dans le développement de $(x-a)(x-a^2)\ldots.(x-a^{t-1})$.

Montrons maintenant qu'il existe des modules u pour lesquels la congruence

$$X(x)\equiv 0 \pmod{u}$$

est possible. En premier lieu, si u est égal à un nombre premier q tel que t divise $\psi(q)$, l'égalité

$$x^t = 1 \qquad (\text{gr. } Q)$$

où Q désigne le groupe formé par l'ensemble de tous les nombres positifs premiers à q et non supérieurs à q, admet nécessairement une solution a différente de l'élément-unité. L'expression

$$a^t - 1 = (a-1)X(a)$$

sera alors divisible par q. Or nous savons que la divisibilité d'un produit par un nombre premier suppose la divisibilité d'au moins un des facteurs par ce nombre premier.* La solution a étant différente de 1, la différence $a-1$ ne peut être divisible par q; c'est donc le facteur $X(a)$ qui doit l'être et l'on aura

$$X(a)\equiv 0 \pmod{q}.$$

De même, si le module u est égal à une puissance q^w d'un nombre premier q pour lequel t divise $\psi(q)$, la congruence

$$X(x)\equiv 0 \pmod{q^w}$$

admet nécessairement une solution. En effet, soit b une solution de la congruence

$$x^t\equiv 1 \pmod{q}$$

différente de l'unité, on aura

$$X(b)\equiv 0 \pmod{q}.$$

Désignons par $q^\varkappa$ la plus haute puissance de q qui divise $X(b)$, si $\varkappa \geqq w$, en peut faire $a=b$, si non posons

$$b^t\equiv 1+hq^\varkappa \pmod{q^{\varkappa+1}}$$

ce qu'on peut toujours faire en vertu de ce que $b^t-1=(b-1)X(b)$ est divisible par $q^\varkappa$. Je dis que h n'est pas divisible par q, car dans le cas contraire $b^t-1=(b-1)X(b)$ serait divisible par $q^{\varkappa+1}$ et comme $b-1$ n'est pas divisible

* Euclidis Elementa, ed. Heiberg VII, 30, t. II, p. 248.

par q, $X(b)$ serait divisible par $q^{\kappa+1}$ contrairement à la supposition. On aura maintenant pour toute valeur de k

$$(b+kq^{\kappa})^t \equiv 1 + hq^{\kappa} + tb^{t-1}kq^{\kappa} \pmod{q^{\kappa+1}}.$$

Je pose maintenant

$$h + ktb^{t-1} \equiv 0 \pmod{q}$$

et je détermine k par cette congruence ce qui est toujours possible car t ne peut avoir un facteur commun avec q que dans le cas où $t=q$; or dans ce cas t ne pourrait diviser $\psi(q)$, les nombres premiers à q et non supérieurs à q devant être cherchés dans la suite

$$1, 2, \ldots . q-1.$$

Le nombre k étant ainsi choisi, on aura

$$(b+kq^{\kappa})^t \equiv 1 \pmod{q^{\kappa+1}}$$

et l'expression

$$(b+kq^{\kappa})^t - 1 = (b+kq^{\kappa}-1)\, X(b+kq^{\kappa})$$

sera ainsi divisible par $q^{\kappa+1}$. Comme $b+kq^{\kappa}-1$ n'est pas divisible par q, on aura

$$X(b+kq^{\kappa}) \equiv 0 \pmod{q^{\kappa+1}}.$$

Le nombre k étant premier à q et si l'on veut non supérieur à q, l'expression $b+kq^{\kappa}$ sera première à $q^{\kappa+1}$ et non supérieure à $q^{\kappa+1}$. En procédant ainsi de proche en proche, on trouvera une solution a de la congruence

$$X(x) \equiv 0 \pmod{q^{\kappa+1}}$$

première à $q^{\kappa+1}$ et non supérieure à $q^{\kappa+1}$.

D'une manière générale, si l'on a

$$u = q_1^{w_1} q_2^{w_2} \ldots . q_v^{w_v}$$

où t divise tous les nombres

$$\psi(q_1), \psi(q_2), \ldots . \psi(q_v)$$

les nombres $q_1, q_2, \ldots . q_v$ étant d'ailleurs des nombres premiers différents entre eux, on peut trouver une solution a de la congruence

$$X(x) \equiv 0 \pmod{u}$$

et par suite effectuer la décomposition

$$X(x) \equiv (x-a)(x-a^2) \ldots . (x-a^{t-1}) \pmod{u}.$$

En effet, si a_1 est une solution de l'égalité

$$X(x) \equiv 0 \pmod{q_1^{w_1}}$$

a_2 une solution de l'égalité

$$X(x) \equiv 0 \pmod{q_2^{w_2}},$$

. . . .

enfin a_v une solution de l'égalité

$$X(x) \equiv 0 \pmod{q_v^{w_v}}$$

on n'aura qu'à faire*

$$\begin{aligned} a &\equiv a_1 \pmod{q_1^{w_1}}, \\ a &\equiv a_2 \pmod{q_2^{w_2}}, \\ &\dots\dots\dots\dots \\ a &\equiv a_v \pmod{q_v^{w_v}} \end{aligned}$$

et l'on aura

$$X(a) \equiv 0 \pmod{u}$$

et par suite

$$X(x) \equiv (x-a)(x-a^2)\dots(x-a^{t-1}) \pmod{u}.$$

Il est facile d'évaluer le nombre des solutions de la congruence

$$x^t \equiv 1 \pmod{u}$$

pour tout module u de la forme $q_1^{w_1} q_2^{w_2} \dots q_v^{w_v}$ où $q_1, q_2, \dots q_v$ sont des nombres premiers différents tels que t divise tous les $\psi(q)$. En effet, pour $u = q$ on aura

$$x^t - 1 \equiv (x-1)(x-a)(x-a^2)\dots(x-a^{t-1}) \pmod{q}.$$

Or un produit ne peut être divisible par un nombre premier à moins qu'un des facteurs ne le soit; on aura donc les solutions

$$\begin{aligned} x &\equiv 1 \pmod{q}, \\ x &\equiv a \pmod{q}, \\ x &\equiv a^2 \pmod{q}, \\ &\dots\dots\dots\dots \\ x &\equiv a^{t-1} \pmod{q}. \end{aligned}$$

Ces solutions sont d'ailleurs toutes différentes entre elles, car si l'on avait

$$a^h \equiv a^k \pmod{q},$$

par exemple, où h et k sont des nombres différents pris dans la suite

$$0, 1, 2, \dots t-1$$

* Disquisitiones arithmeticae, art. 36.

et $h > k$, on en tirerait

$$a^{h-k} \equiv 1 \pmod{q}$$

contrairement à la supposition que a appartient à l'exposant t. Quand on a

$$u = q^w$$

on a encore

$$x^t - 1 = (x-1)(x-a)(x-a^2) \ldots . (x-a^{t-1}) \pmod{q^w}$$

et comme deux facteurs de ce produit ne peuvent pas être divisible par q en même temps, comme nous venons de le voir, il faut qu'un des facteurs soit divisible par q^w. On en tire les seules et uniques solutions

$$\begin{aligned} x &\equiv 1 \pmod{q^w}, \\ x &\equiv a \pmod{q^w}, \\ x &\equiv a^2 \pmod{q^w}, \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a^{t-1} \pmod{q^w} \end{aligned}$$

qui seront encore différentes entre elles. Le nombre des solutions de la congruence

$$x^t \equiv 1 \pmod{q^w}$$

est donc égal à t. Enfin pour

$$u = q_1^{w_1} q_2^{w_2} \ldots . q_v^{w_v}$$

ou aura de même

$$x^t - 1 \equiv (x-1)(x-a)(x-a^2) \ldots . (x-a^{t-1}) \pmod{u}.$$

Or comme deux facteurs du produit précédent ne peuvent être divisible en même temps par un même nombre premier q, il s'agit de distribuer toutes les puissances de nombre premier q^w parmi les facteurs du produit

$$(x-1)(x-a)(x-a^2) \ldots . (x-a^{t-1})$$

avec la faculté d'attribuer plusieurs puissances de nombre premier à un seul facteur. Comme il y a ainsi t alternatives pour chaque puissance de nombre premier, cela nous donne en tout

$$t^v$$

solutions, qui seront d'ailleurs toutes différentes entre elles, en vertu de l'article 36 des *Disquisitiones arithmeticae*.

Il existe des modules pour lesquels la décomposition de $X(x)$ en facteurs linéaires est impossible, En effet, posons d'abord

$$u = t$$

et désignons par T le groupe formé par l'ensemble des nombres premiers à t et non supérieurs à t, l'égalité

$$x^t = 1 \quad (\text{gr. } T)$$

n'admettra qu'une seule et unique solution

$$x = 1 \quad (\text{gr. } T)$$

car $\psi(t)$ n'est pas divisible par t. De même la congruence

$$x^t \equiv 1 \quad (\text{mod. } t)$$

n'aura qu'une seule et unique solution

$$x \equiv 1 \quad (\text{mod. } t).$$

Or comme on a $X(1) = t \equiv 0 \quad (\text{mod. } t)$

on aura la décomposition

$$X(x) \equiv (x-1)^{t-1} \quad (\text{mod. } t)$$

et par suite $x^t - 1 \equiv (x-1)^t \quad (\text{mod. } t).$

Mais quand $u = t^\tau$

où $\tau > 1$, la congruence

$$X(x) \equiv 0 \quad (\text{mod. } t^\tau)$$

n'admet pas de solution et par suite n'est pas décomposable en un produit de facteurs linéaires. En effet, si l'on avait

$$X(a) \equiv 0 \quad (\text{mod. } t^\tau)$$

on en tirerait

$$X(x) \equiv (x-a)(x-a^2)\ldots\ldots(x-a^{t-1}) \quad (\text{mod. } t^\tau)$$

et par suite

$$X(1) \equiv (1-a)(1-a^2)\ldots\ldots(1-a^{t-1}) \quad (\text{mod. } t^\tau).$$

On devrait donc avoir, pour une certaine valeur de h comprise entre 1 et $t-1$ inclusivement

$$a^h \equiv 1 \quad (\text{mod. } t)$$

et par suite

$$a^{mh+nt} \equiv 1 \quad (\text{mod. } t)$$

où m et n sont des nombres entiers quélconques. On en tirerait

$$a^k \equiv 1 \pmod{t}$$

pour toute valeur de k prise dans la suite

$$1, 2, \ldots . t-1$$

et par suite

$$t \equiv t^{t-1} \pmod{t^\tau}$$

congruence absurde puisque tant $t-1$ què τ sont supérieurs à l'unité. La congruence

$$x^t \equiv 1 \pmod{t^\tau}$$

admet t solutions et pas plus car $\psi(t^\tau)$ est divisible par t et pas par une puissance supérieure de t. Or comme on a

$$x^t - 1 = (x-1) X(x)$$

on voit facilement que ces solutions sont

$$1, 1 + t^{\tau-1}, 1 + 2t^{\tau-1}, \ldots , 1 + (t-1) t^{\tau-1}$$

car toutes ces valeurs rendent $x-1$ divisible par $t^{\tau-1}$ et $X(x)$ divisible par t. Toutes ces solutions étant différentes entre elles, il ne pourra y en avoir d'autres. Il est clair que si l'on pose

$$a = 1 + kt^{\tau-1}$$

où k est pris dans la suite

$$1, 2, \ldots . t-1$$

toutes les solutions de la congruence

$$x^t \equiv 1 \pmod{t^\tau}$$

seront

$$1, a, a^2, \ldots . a^{t-1}.$$

Mais on ne peut plus parler d'une décomposition telle que

$$x^t - 1 \equiv (x-1)(x-a)(x-a^2) \ldots . (x-a^{t-1}) \pmod{t^\tau}$$

car

$$1 + a + a^2 + \ldots . a^{t-1}$$

est bien divisible par t mais non par t^2.

La congruence

$$X(x) \equiv 0 \pmod{u}$$

n'est pas résoluble non plus quand le module est égal à un nombre premier r différent de t et tel que t ne divise pas $\psi(r)$. En effet, si l'on désigne par R le

groupe formé par l'ensemble des nombres premiers à r et non supérieurs à r, l'égalité

$$x^t = 1 \qquad (\text{gr. } R)$$

n'admettra qu'une seule solution

$$x = 1.$$

De même la congruence

$$x^t \equiv 1 \qquad (\text{mod. } r)$$

n'admettra qu'une seule et unique solution

$$x \equiv 1 \qquad (\text{mod. } r).$$

Or comme on a

$$X(1) = t$$

la congruence

$$X(x) \equiv 0 \qquad (\text{mod. } r)$$

n'admet pas la solution

$$x \equiv 1 \qquad (\text{mod. } r)$$

et par suite elle n'en admettra aucune puisque toute solution de la congruence

$$X(x) \equiv 0 \qquad (\text{mod. } r)$$

est nécessairement une solution de la congruence

$$x^t - 1 \equiv 0 \qquad (\text{mod. } r).$$

On ne peut parler dans ce cas non plus d'une décomposition telle que

$$x^t - 1 \equiv (x-1)^t \qquad (\text{mod. } r)$$

car le coefficient de x^{t-1} dans le développement de $(x-1)^t$ est égal à $-t$ et par suite non divisible par r. D'une manière générale, la congruence

$$X(x) \equiv 0 \qquad (\text{mod. } u)$$

n'admet pas de solution et est indécomposable en facteurs linéaires pour tout module u divisible par un nombre premier r différent de t et tel que $\psi(r)$ n'est pas divisible par t. En somme, la congruence

$$X(x) \equiv 0 \qquad (\text{mod. } u)$$

est résoluble et par suite décomposable en un produit de facteurs linéaires pour tout module u qui n'est divisible ni par t^2 ni par aucun nombre premier r différent de t et tel que t ne divise pas $\psi(r)$. En effet, un tel module u est soit de la forme

$$u = q_1^{w_1} q_2^{w_2} \ldots . q_v^{w_v}$$

où t divise tous les $\psi(q)$, soit de la forme

$$u = t q_1^{w_1} q_2^{w_2} \ldots . q_v^{w_v}$$

où t divise encore tous les $\psi(q)$. Dans le premier cas on n'a qu'à faire

$$a \equiv a_k \qquad (\text{mod. } q_k^{w_k}) \qquad (k = 1, 2, \ldots . v)$$

et dans le second

$$a \equiv 1 \qquad (\text{mod. } t),$$
$$a \equiv a_k \qquad (\text{mod. } q_k^{w_k}) \qquad (k = 1, 2, \ldots . v)$$

et l'on aura

$$X(x) \equiv (x - a)(x - a^2) \ldots . (x - a^{t-1}) \qquad (\text{mod. } u).$$

Tout nombre M qui n'est divisible ni par t^2 ni par un nombre premier r différent de t et tel que t ne divise pas $\psi(r)$, peut donc être appelé *diviseur de* $X(x)$.

Cela étant ainsi, désignons par Ξ_1 le groupe formé par l'ensemble de toutes les solutions de l'égalité

$$x^t = 1 \qquad (\text{gr. } U)$$

et par t^{m_1} son ordre, il est facile d'évaluer m_1. En effet, posons

$$u = t^\tau MN$$

où t^τ est la plus haute puissance de t qui divise u, le nombre τ pouvant d'ailleurs avoir la valeur 0, et M le produit de tous les diviseurs premiers q de $\frac{u}{t^\tau}$ tels que t divise $\psi(q)$, chaque nombre premier q devant d'ailleurs figurer dans M autant de fois que dans u. Le nombre N n'est donc autre chose que le quotient $\frac{u}{t^\tau M}$ qui peut se réduire éventuellement à un. Si l'on désigne par v le nombre de nombres premiers différents qui divisent M, la congruence

$$x^t \equiv 1 \qquad (\text{mod. } M)$$

admettra, comme nous l'avons vu, t^v solutions. La congruence

$$x^t \equiv 1 \qquad (\text{mod. } t^\tau)$$

admettra une seule solution dans le cas où $\tau < 2$ et en admettra t dans le cas où $\tau > 1$. Enfin si $N > 1$, la congruence

$$x^t \equiv 1 \qquad (\text{mod. } N)$$

n'admet qu'une seule et unique solution, car t ne divise pas $\psi(N)$. Cela étant ainsi, en vertu de l'article 36 des *Disquisitiones arithmeticae* on aura

$$m_1 = v + \varepsilon$$

où ε est égal à 1 dans le cas où $\tau > 1$, il est égal à 0 dans tous les autres cas. Le groupe Ξ_1 est donc à $m_1 = v + \varepsilon$ bases où le nombre m_1 ne peut jamais surpasser le nombre de nombres premiers différents divisant u. Disons plus, comme on a

$$\psi(2^z) = 2^{z-1}$$

pour toute valeur positive et entière de z, le nombre m_1 ne peut jamais surpasser le nombre de nombres premiers impairs divisant u. Nous avons supposé le nombre u décomposé en un produit de la forme

$$t^\tau MN,$$

mais la théorie elle-même nous fournit cette décomposition. En effet, il résulte de la théorie précédente que le moindre commun multiple de tous les plus grands communs diviseurs de

$$X(x) \text{ et } u,$$

où x doit parcourir toutes les solutions de

$$x^t \equiv 1 \pmod{u},$$

est égal à tM ou à M suivant que τ est plus grand ou égal à 0. D'une manière analogue, la théorie elle-même nous fournit la décomposition de M en un produit de puissances de nombre premier premières entre elles. Il y a une différence essentielle entre le postulat III d'Euclide,* par exemple, et la supposition qu'on fait dès le début de la théorie des formes quadratiques qu'il est possible d'effectuer la décomposition de tout nombre donné en ses facteurs premiers. Le postulat III ne regoit aucun perfectionnement à mesure qu'on avance dans la géométrie. Il n'en est pas de même de la décomposition d'un nombre en ses facteurs premiers. D'abord ce n'est qu'un tâtonnement fort rude, mais il le devient beaucoup moins à mesure qu'on avance dans la théorie des formes quadratiques. Il est donc de toute nécessité d'y revenir, une fois la théorie des formes quadratiques achevée. La sixième section des *Disquisitiones arithmeticae* n'est pas un hors-d'œuvre, c'est un complément absolument indispensable de toute théorie des formes quadratiques. Que l'on ramène la question qui consiste à déterminer le caractère quadratique d'un nombre donné a par rapport à un nombre donné m à la décomposition de m en ses facteurs premiers, je le veux bien. Mais cela fait,

---

* Elementa, ed. Heiberg, t. I, p. 8.

que l'on complète la théorie en montrant comment la décomposition de m en ses facteurs premiers dépend de la résolution de la congruence

$$x^2 \equiv a \pmod{m}.$$

Abordons maintenant la congruence*

$$x^2 \equiv 1 \pmod{u}.$$

Ici, il se présente quelque chose de particulier. En effet, l'expression $x^2 - 1$ est décomposable en facteurs linéaires algebriquement, car on a

$$x^2 - 1 = (x-1)(x+1).$$

On aura donc

$$x^2 - 1 \equiv (x-1)(x-u+1) \pmod{u}$$

où $u-1$ est, comme il est facile de voir, premier à u. S'il s'agit de rendre $x^2 - 1$ divisible par u, il suffit donc de rendre $x-1$ divisible par un diviseur h de u et $x-u+1$ divisible par un diviseur k de u tels qu'on ait

$$hk \equiv 0 \pmod{u}.$$

Je dis que h et k ne peuvent avoir d'autre facteur commun que 2. En effet, cela résulte immédiatement de la relation

$$(x-1)-(x-u+1)+u = 2.$$

Si donc le module u est impair, les nombres h et k ne peuvent avoir de facteur commun. Pour tout module u supérieur à 2, la congruence a d'ailleurs deux solutions bien distinctes

$$x \equiv 1 \pmod{u}$$

et

$$x \equiv u-1 \pmod{u}.$$

D'où il résulte que 2 divise toujours $\psi(u)$ quelque soit le module u supérieur à 2. Si le module u est égal à une puissance de nombre premier impair q^w, la congruence

$$x^2 \equiv 1 \pmod{q^w}$$

n'a que deux solutions. En effet, le plus grand commun diviseur de $x-1$, $x-q^w+1$ et q étant égal 1 quelle que soit la valeur de x, il faut qu'un des deux facteurs $x-1$ et $x-q^w+1$ soit divisible par q^w pour que x^2-1 le soit, ce qui donne les deux seules et uniques solutions

$$x \equiv 1 \pmod{q^w},$$
$$x \equiv q^w - 1 \pmod{q^w}.$$

* Cette congruence a déjà été considérée par M. Schering dans son mémoire intitulé *Zur Theorie der quadratischen Reste* (Acta Mathematica, Vol. I, p. 153).

Quand on a $$u = q_1^{w_1} q_2^{w_2} \dots . q_v^{w_v}$$
où $$q_1^{w_1},\ q_2^{w_2},\ \dots .\ q_v^{w_v}$$
sont des puissances de nombre premier impair premières entre elles, on établira comme dans le cas de la congruence
$$x^t \equiv 1 \pmod{u}$$
que la congruence $$x^2 \equiv 1 \pmod{u}$$
admet 2^v solutions.

Considérons maintenant la congruence
$$x^2 \equiv 1 \pmod{2^z}.$$
Si $z = 1$, elle n'admet évidemment qu'une seule et unique solution
$$x \equiv 1 \pmod{2}.$$
Si $z = 2$, on a les solutions
$$x \equiv 1 \pmod{4},$$
$$x \equiv 3 \pmod{4}.$$
Comme ces solutions épuisent les nombres premiers à 4 et non supérieurs à 4, il ne pourra y en avoir d'autres. Nous pouvons donc nous borner à la considération du cas où $z > 2$. On aura donc la congruence
$$x^2 - 1 \equiv (x-1)(x - 2^z + 1) \equiv 0 \pmod{2^z}.$$
Comme on a $$(x - 2^z + 1) - (x - 1) \equiv 2 \pmod{2^z}$$
pour toute valeur de x, il est clair qu'un des deux nombres $x - 2^z + 1$ et $x - 1$ sera pairement pair et l'autre impairement pair pour toute valeur de x qui satisfait à la congruence
$$x^2 \equiv 1 \pmod{2^z}.$$
Le nombre pairement pair devra donc être divisible par 2^{z-1} et il sera par conséquent $\equiv 0$ ou $\equiv 2^{z-1} \pmod{2^z}$.

Cela nous donne en tout quatre solutions
$$x \equiv 1 \pmod{2^z},$$
$$x \equiv 1 + 2^{z-1} \pmod{2^z},$$
$$x \equiv 2^z - 1 \pmod{2^z},$$
$$x \equiv 2^{z-1} - 1 \pmod{2^z}.$$
Toutes ces solutions sont distinctes entre elles, comme on peut s'en assurer en évaluant (mod. 2^z) leurs différences deux à deux. En vertu de l'article 36 des

Disquisitiones arithmeticae que nous avons déjà cité, tant de fois, on aura donc la proposition suivante. La congruence

$$x^2 \equiv 1 \pmod{u}$$

admet 2^v solutions, si u est un nombre impair ou impairement pair divisible par v nombres premiers impairs différents. Le nombre de solutions est égal à 2^{v+1} si le nombre u est divisible par 4 sans l'être par 8, enfin le nombre de solutions est égal à 2^{v+2} quand le module u est divisible par 8.

La différence essentielle entre la congruence

$$x^2 \equiv 1 \pmod{u}$$

et la congruence $$x^t \equiv 1 \pmod{u}$$

où t est un nombre premier impair, consiste donc en ce que $x^t - 1$ n'est pas décomposable en facteurs linéaires pour $u = t^\tau$ où $\tau > 1$, tandis que $x^2 - 1$ est algébriquement décomposable en facteurs linéaires et par suite aussi pour le module 2^z.

En résumé, si l'on désigne par Ξ_1 le groupe formé par l'ensemble des solutions de la congruence

$$x^s \equiv 1 \pmod{u}$$

où s est un nombre premier quelconque et par s^{m_1} son ordre, on aura, si

$$u = s^\sigma q_1^{w_1} q_2^{w_2} \ldots . q_v^{w_v}$$

est la décomposition de u en puissances de nombre premier premières entre elles (la puissance s^σ pouvant se réduire éventuellement à l'unité),

$$m_1 = v$$

pour $s = 2$ $\sigma < 2$,

$$m_1 = v + 1$$

pour $s = 2$ $\sigma = 2$,

$$m_1 = v + 2$$

pour $s = 2$ $\sigma > 2$,

$$m_1 = v_t$$

pour $s = t > 2$, où v_t désigne le nombre des nombres de la suite

$$\psi(s^\sigma),\ \psi(q_1^{w_1}),\ \psi(q_2^{w_2}) \ldots . \psi(q_v^{w_v})$$

qui sont divisibles par s de sorte qu'on aura toujours

$$v_t \leqq v'$$

si l'on désigne par v' le nombre de nombres premiers impairs qui divisent u. Le groupe U sera par conséquent à autant de bases que le groupe formé par l'ensemble des solutions de la congruence

$$x^2 \equiv 1 \pmod{u}.$$

27.

Passons maintenant au théorème d'Euclide.* Si les nombres premiers étaient en nombre fini et se réduisaient par exemple aux nombres premiers

$$q_1, \ q_2, \ldots . \ q_n$$

qu'on peut supposer rangés par ordre de grandeur, le nombre $q_1 q_2 \ldots . \ q_n + 1$ serait ou premier ou divisible par un nombre premier $q_{n+1} > q_n$. Il résulte du raisonnement d'Euclide que, entre q_n exclusivement et $q_1 q_2 \ldots . \ q_n + 1$ inclusivement il existe au moins un nombre premier.

Voyons maintenant si, en se fondant sur les préliminaires établis dans les paragraphes précédents, il est possible de conclure quelque chose de plus.

Posons $$M = q_1 q_2 \ldots . \ q_n$$

le groupe formé par tous les nombres premiers à M et non supérieurs à M sera à $n - 1$ bases. Or si l'on désigne par

$$q_{n+1}, \ q_{n+2}, \ldots . \ q_{n+h}$$

tous les nombres premiers compris entre q_n exclusivement et M, tous les nombres qui font partie du groupe $\mathfrak{M}$ pourront être représentés par la formule

$$q_{n+1}^{u_{n+1}} q_{n+2}^{u_{n+2}} \ldots . \ q_{n+h}^{u_{n+h}}$$

où les nombres u ont la valeur 0 ou une valeur entière positive. Il s'ensuit qu'on doit avoir, comme nous l'avons démontré dans les paragraphes précédents,

$$h \geqq n - 1.$$

Entre q_n exclusivement et M, il existe donc au moins $n - 1$ nombres premiers. Si, dans le raisonnement d'Euclide, on remplace $M + 1$ par $M - 1$, il en résultera qu'entre q_n exclusivement et M, il existe au moins un seul nombre premier. La démonstration de M. Kummer (Monatsberichte der Berliner Academie) repose sur des considérations analogues à celles que nous venons de développer. M. Kummer

---

* Elem. IX, 20, ed. Heiberg, Vol. II, p. 388.

démontre d'abord que l'ensemble $\mathfrak{M}$ renferme au moins un élément et que par suite il faut au moins un nombre premier différent de

$$q_1, q_2, \dots q_n$$

pour qu'on puisse l'exprimer comme un produit de facteurs premiers. La démonstration du théorème d'Euclide que j'ai donnée il y a huit ans dans le *Bulletin de M. Darboux* repose sur d'autres principes. Il est facile de faire voir que dans la suite

$$1, 2, 3, \dots N$$

il y a plus de $\frac{1}{3}N$ nombres sans facteur quadratique. Si donc on désigne par

$$q_1, q_2, \dots q_m$$

les nombres premiers de la suite précédente, tout nombre sans facteur quadratique de la suite sera de la forme

$$q_1^{u_1} q_2^{u_2} \dots q_m^{u_m}$$

où tout exposant u_k a une des deux valeurs 0 et 1. Comme cette fois-ci les exposants des nombres premiers ont une limite supérieure, il n'est plus nécessaire de recourir à la théorie des groupes eulériens et l'on obtient immédiatement

$$m > \text{log. acoust.} \tfrac{1}{3} N.$$

28.

Le raisonnement d'Euclide peut servir à démontrer l'existence de nombres premiers ayant certaines formes particulières données d'avance. Nous avons vu que t étant un nombre premier impair quelconque, l'expression

$$\frac{x^t - 1}{x - 1} = X(x) = x^{t-1} + x^{t-2} + \dots + x + 1$$

ne peut admettre comme diviseurs premiers que le nombre premier t et cela une seule fois, et des nombres premiers de la forme

$$ht + 1$$

où h est un nombre entier positif quelconque. En particulier, $X(t)$ n'étant pas divisible par t et étant supérieur à l'unité, sera nécessairement divisible par un nombre premier q_1 de la forme $ht + 1$. De même $X(tq_1)$ étant supérieur à 1 et n'étant divisible ni par t ni par q_1 sera nécessairement divisible par un nombre premier q_2 de la forme $ht + 1$ et différent de q_1. D'une manière analogue le

nombre $X(tq_1q_2)$ étant supérieur à 1 et n'étant divisible ni par t, ni par q_1 ni par q_2 sera divisible par un nombre premier q_3 de la forme $ht+1$ et différent tant de q_1 que de q_2.

En continuant de la même manière on peut trouver autant de nombres premiers de la forme $ht+1$

$$q_1, q_2, \ldots . q_n$$

que l'on veut. Il est donc bien démontré que le nombre de nombres premiers de la forme $ht+1$ peut surpasser tout nombre entier donné d'avance.* Nous avons supposé t impair; si l'on met dans la formule $ht+1$ à la place de t le seul et unique nombre premier pair 2, on obtient la formule

$$2h+1$$

qui convient à tout nombre premier impair. La proposition s'applique donc aussi à ce cas. Il convient maintenant de dire quelques mots sur les classes de nombres premiers de M. Lipschitz.† Le nombre premier 2 forme à lui seul la classe 1, à la classe 2 appartiennent tous les nombres premiers de la forme 2^n+1 et d'une manière générale on considère comme appartenant à la classe μ tout nombre premier q_μ tel que $q_\mu - 1$ est divisible par un nombre premier de la classe $\mu - 1$ et ne contient d'autres diviseurs premiers que des nombres premiers des $\mu - 1$ premières classes.

Le nombre de classes de M. Lipschitz peut surpasser tout nombre entier donné d'avance, car si q_μ est un nombre premier de la classe μ, tout nombre premier de la forme $hq_\mu + 1$, où h est un nombre entier positif, appartiendra évidemment à une classe $\mu + k$ où $k > 0$.

29.

Soient s un nombre premier quelconque et μ un nombre entier positif supérieur à un, on aura

$$\frac{x^{s^\mu}-1}{x^{s^{\mu-1}}-1} = x^{(s-1)s^{\mu-1}} + x^{(s-2)s^{\mu-1}} + \ldots . + x^{s^{\mu-1}} + 1 \equiv s \, (\text{mod. } x^{s^{\mu-1}} - 1)$$

---

* J'ignore l'auteur de cette démonstration.

† Tout ce qui suit jusqu'à la fin de ce paragraphe a été ajouté après l'apparition du beau travail de M. Lipschitz (Journal für Mathematik, Bd. CV, p. 127-156).

quelle que soit la valeur entière de x. Il s'ensuit que tout diviseur premier q de $\frac{x^{s^\mu}-1}{x^{s^{\mu-1}}-1}$ autre que s est premier à $x^{s^{\mu-1}}-1$. On aura donc

$$x^{s^\mu} \equiv 1 \quad (\text{mod. } q),$$

mais non

$$x^{s^{\mu-1}} \equiv 1 \quad (\text{mod. } q)$$

ce qui fait voir que x appartient à l'exposant s^μ (mod. q). Le nombre $\Phi(q) = q - 1$ doit donc être divisible par s^μ et q est par conséquent de la forme $hs^\mu + 1$ où h est un nombre entier positif. Le nombre $\frac{s^{s^\mu}-1}{s^{s^{\mu-1}}-1}$ étant supérieur à l'unité admettra nécessairement un diviseur premier q_1 qui sera différent de s et par suite de la forme $hs^\mu + 1$. Le nombre $\frac{(q_1 s)^{s^\mu}-1}{(q_1 s)^{s^{\mu-1}}-1}$ admettra un diviseur premier q_2 différent de s et q_1 et par suite de la forme $hs^\mu + 1$. De même le nombre $\frac{(q_1 q_2 s)^{s^\mu}-1}{(q_1 q_2 s)^{s^{\mu-1}}-1}$ admettra un diviseur premier q_3 différent de s, q_1 et q_2 et par suite de la forme $hs^\mu + 1$. En continuant de la même manière on peut former autant de nombres premiers de la forme $hs^\mu + 1$ que l'on veut.

Soit maintenant q_1 un nombre premier de la forme $hs^\theta + 1$ obtenu par le procédé qu'on vient d'exposer, désignons par $A_1^{s^\theta}$ le groupe formé par l'ensemble des solutions de la congruence

$$x^{s^\theta} \equiv 1 \quad (\text{mod. } q_1).$$

Nous avons vu dans le §26 que le nombre des solutions de la congruence

$$x^s \equiv 1 \quad (\text{mod. } q_1)$$

est égal à s, il s'ensuit que le groupe $A_1^{s^\theta}$ est monobase et comme il résulte de la formation même du nombre premier q_1 que le groupe $A_1^{s^\theta}$ renferme au moins un élément appartenant à l'exposant s^θ, il est clair que l'ordre du groupe $A_1^{s^\theta}$ sera égal à s^θ. Formons d'une manière analogue un autre groupe monobase A_2^s d'ordre s^θ à l'aide d'un nombre premier q_2 différent de q_1 et ainsi de suite jusqu'à un certain groupe monobase $A_{m_\theta}^{s^\theta}$ d'ordre s^θ qu'on formera à l'aide d'un nombre premier q_{m_θ} différent des nombres premiers

$$q_1, q_2, q_3, \ldots q_{m_\theta - 1}.$$

Formons d'une manière analogue un certain nombre $m_{\theta-1} - m_\theta$ de groupes monobases

$$A_{m_\theta+1}^{s^{\theta-1}}, A_{m_\theta+2}^{s^{\theta-1}}, \ldots A_{m_\theta-1}^{s^{\theta-1}}$$

d'ordre $s^{\theta-1}$ à l'aide de nombres

$$q_{m_\theta+1},\ q_{m_\theta+2},\ \ldots\ q_{m_{\theta-1}}$$

différents tant entre eux que des nombres premiers

$$q_1,\ q_2,\ \ldots\ q_{m_\theta}.$$

On continuera la même opération jusqu'à ce qu'on aura formé $m_1 - m_2$ groupes monobases d'ordre s

$$A^s_{m_2+1},\ A^s_{m_2+2},\ \ldots\ A_{m_1}$$

à l'aide de nombres premiers

$$q_{m_2+1},\ q_{m_2+2},\ \ldots\ q_{m_1}$$

différents tant entre eux que des nombres premiers

$$q_1,\ q_2,\ \ldots\ q_{m_2}.$$

Je pose maintenant

$$M = q_1 q_2 \ldots q_{m_1}$$

et je remplace tout élément a du groupe $A_1^{s^\theta}$ par un élément a' satisfaisant aux conditions

$$\begin{aligned} a' &\equiv a \quad (\text{mod. } q_1), \\ a' &\equiv 1 \quad (\text{mod. } q_2), \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ a' &\equiv 1 \quad (\text{mod. } q_{m_1}), \\ a' &< M \end{aligned}$$

et de même pour les autres groupes. Cela ne change en rien la nature des groupes A et maintenant tous leurs éléments peuvent être considérés aussi comme faisant partie du groupe $\mathfrak{M}$ formé par l'ensemble de tous les nombres inférieurs à M et premiers à M. Encore plus, si l'on prend deux éléments a et b du groupe $A_1^{s^\theta}$, l'élément c qu'on obtient par la composition des éléments a et b correspondera à l'élément c' du groupe $\mathfrak{M}$, formé par la composition des éléments a' et b' de ce groupe qui correspondent respectivement aux éléments a et b du groupe $A_1^{s^\theta}$. Et de même pour les autres groupes. Cela étant ainsi, je désigne toujours par le signe $A_1^{s^\theta}$ le groupe $A_1^{s^\theta}$ ainsi transformé, et je dis que les groupes

$$A_1^{s^\theta},\ A_2^{s^\theta},\ \ldots\ A^s_{m_1}$$

sont susceptibles d'être combinés en un groupe Ξ_θ. En effet, si l'on désigne par

$$a_1,\ a_2,\ \ldots\ a_{m_1}$$

des éléments appartenant respectivement aux groupes

$$A_1^{s^\theta},\ A_2^{s^\theta},\ \ldots\ldots A_{m_1}^{s}$$

une congruence telle que

$$a_1 \equiv a_2 a_3 \ldots\ldots a_{m_1} \pmod{M}$$

ne peut avoir lieu à moins qu'on ait

$$a_1 \equiv 1 \pmod{M}$$

car on a

$$a_2 \equiv a_3 \equiv \ldots\ldots \equiv a_{m_1} \pmod{q_1}.$$

En posant

$$\Xi_\theta = A_1^{s^\theta} A_2^{s^\theta} \ldots\ldots A_{m_1}^{s}$$

on aura un groupe tout à fait analogue à celui que nous avons étudié sous ce nom dans les paragraphes 7–10.

Soit maintenant E un groupe eulérien quelconque et que sa décomposition en groupes uniprimes d'ordres premiers entre eux, donne

$$E = \Xi_{\theta_1} \Xi_{\theta_2} \ldots\ldots \Xi_{\theta_n}$$

formons à l'aide de nombres

$$M_1,\ M_2,\ \ldots\ldots M_n$$

premiers deux à deux, des groupes

$$H_1,\ H_2,\ \ldots\ldots H_n$$

tout à fait analogues aux groupes

$$\Xi_{\theta_1},\ \Xi_{\theta_2},\ \ldots\ldots \Xi_{\theta_n}.$$

Supposons de plus qu'on ait choisi les éléments du groupe H_1 de manière qu'ils soient tous congrus à un suivant les modules M_2, M_3, ... M_n et de même pour les autres groupes, le groupe

$$F = H_1 H_2 \ldots\ldots H_n \quad (\text{mod. } M = M_1 M_2 \ldots\ldots M_n)$$

sera tout à fait analogue au groupe E.

La théorie des groupes eulériens trouve donc une application complète dans la théorie des restes suivant un module quelconque.

L'application du procédé du géomètre grec à d'autres cas de la proposition de Lejeune Dirichlet sur la progression arithmétique fera l'objet d'un prochain article.

GRA-THUMIAC, le 26 août 1889.